

IX FÓRUM DA INTERNET NO BRASIL – RELATÓRIO DE WORKSHOP

1. INFORMAÇÕES BÁSICAS SOBRE O WORKSHOP

TÍTULO: PROTEÇÃO DE DADOS E SEGURANÇA PÚBLICA NO BRASIL: CONTEXTO REGULATÓRIO ATUAL E PERSPECTIVAS FUTURAS

TEMA: Lei Geral de Proteção de Dados e segurança pública.

FORMATO: Painel.

PROPONENTE:

- **Nome: Gustavo Ramos Rodrigues.**
- Organização: Instituto de Referência em Internet e Sociedade – IRIS.
- Setor: Terceiro Setor.
- Minibiografia: Pesquisador no Instituto de Referência em Internet e Sociedade (IRIS). Bacharel em Antropologia pela Universidade Federal de Minas Gerais (UFMG). Membro do Observatório de Inovação, Cidadania e Tecnociência (InCiTE). Participa da coordenação da Rede de Pesquisa em Governança da Internet (REDE).

PALESTRANTES:

- **Nome: Bruna Martins dos Santos.**
- Organização: Coding Rights.
- Setor: Terceiro Setor.
- Minibiografia: Bacharel em Direito pelo Centro Universitário de Brasília e Analista de policy e advocacy na Coding Rights, onde atua no acompanhamento legislativo para o Radarlegislativo.org com foco em temas como Proteção de Dados Pessoais, Direitos Humanos na Digital e Governança da Internet. Bruna também foi assessora jurídica na Subchefia para Assuntos Jurídicos da Casa Civil da Presidência da República.
- **Nome: Jacqueline de Souza Abreu.**
- Organização: Barroso Fontelles, Barcellos, Mendonça & Associados
- Setor: Privado.
- Minibiografia: Advogada especializada em direito digital e doutoranda na Faculdade de Direito da USP. Mestre em direito pela University of California, Berkeley (EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Alemanha), com foco em direitos fundamentais. Advogada no escritório Barroso Fontelles, Barcellos, Mendonça & Associados.
- **Nome: Milena Santana de Araújo Lima.**
- Organização: Polícia Civil do Estado do Tocantins.

- Setor: Governamental.
- Minibiografia: Delegada de Polícia Civil com atuação junto ao TJTO, ex-titular da DRCC/PCTO, tendo atuação anterior na DINT da Senasp-MJ e na Polícia Civil de Sergipe. Possui graduação em Direito, pós-graduação e especialização em cybercrimes. Ministrado aulas de investigação em meios digitais na Escola da Magistratura Tocantinense, CESAFA do Ministério Público de Tocantins, Escola Superior da PCTO, entre outros.
- **Nome: Paulo Rená da Silva Santarém.**
- Organização: Instituto Beta para Internet e Democracia.
- Setor: Comunidade Científica e Tecnológica.
- Minibiografia: Mestre em Direito, Estado e Constituição e especialista em Direito Constitucional do Trabalho pela Universidade de Brasília. Assessor jurídico do Tribunal Superior do Trabalho. Professor da Faculdade de Direito do UniCEUB.

MODERADOR:

- **Nome: Gustavo Ramos Rodrigues.**
- Organização: Instituto de Referência em Internet e Sociedade – IRIS.
- Setor: Terceiro Setor.
- Minibiografia: Pesquisador no Instituto de Referência em Internet e Sociedade (IRIS). Bacharel em Antropologia pela Universidade Federal de Minas Gerais (UFMG). Membro do Observatório de Inovação, Cidadania e Tecnocência (InCiTE). Participa da coordenação da Rede de Pesquisa em Governança da Internet (REDE).

RELATOR:

- **Nome: Victor Araújo de Menezes.**
- Organização: Universidade Federal de Santa Catarina.
- Setor: Comunidade Científica e Tecnológica.

2. ESTRUTURAÇÃO DO WORKSHOP

O workshop “PROTEÇÃO DE DADOS E SEGURANÇA PÚBLICA NO BRASIL: CONTEXTO REGULATÓRIO ATUAL E PERSPECTIVAS FUTURAS” buscou apresentar e discutir o contexto regulatório nacional referente ao tratamento de dados pessoais para fins de segurança pública, investigações criminais e repressão de infrações penais.

Dois eixos temáticos principais estruturaram as exposições: i) as normas aplicáveis à matéria no presente, suas limitações e possibilidades; ii) perspectivas e desafios de uma legislação específica para o setor securitário, a qual é prevista pela Lei Geral de Proteção de Dados.

As perguntas que serviram como orientadoras para a discussão foram:

1. Quais os instrumentos legais presentemente aplicáveis ao tratamento de dados pessoais para fins de segurança pública, investigações criminais e repressão de infrações penais? Qual sua eficácia em equilibrar a tutela dos direitos dos titulares e as necessidades do setor?

2. Considerando que a LGPD exclui o tratamento para essas finalidades de seu escopo de aplicação e prevê a elaboração de norma específica para tanto, quais modelos regulatórios disponíveis em outras jurisdições podem servir como inspiração para essa norma?

A justificativa para a presente discussão em relação à governança da Internet se dá na medida em que, faltando alguns meses para o início da vigência da Lei Geral de Proteção de Dados, é necessário verificar como ela será efetivamente aplicada nas mais determinadas áreas, e quais problemas podem surgir tendo em vista a legislação vigente e as normas aprovadas.

A área de segurança pública é marcada pelo uso crescente das tecnologias de informação, gerando diversas questões como as implicações para operações massivas de tratamentos de dados pessoais, obrigações dos controladores vs. direitos dos titulares, e questões de reconhecimento facial em locais públicos.

Do ponto de vista regulatório, há pouca nitidez na intersecção entre proteção de dados e segurança pública. No Artigo 4º da Lei Geral de Proteção de Dados, existe a previsão de que haverá uma legislação específica para este fim, que “deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei”.

Neste cenário de uma legislação específica futura surgem mais perguntas, que também nortearam a discussão: a) quais instrumentos regulatórios são aplicáveis quando há tratamento para fins exclusivos de segurança pública? b) em que medida essas normas equilibram os direitos dos titulares e as obrigações dos controladores e as necessidades do setor de segurança? c) quais tipos de normas nós queremos para o futuro?

Como metodologia e formas de participação, os panelistas apresentaram slides selecionando pontos específicos sobre a discussão para a realização de um debate posterior, resgatando as questões mais relevantes e também respondendo perguntas da plateia.

Durante a realização do workshop, foram atingidos os objetivos orientadores de levantamento dos problemas relativos à regulação de dados pessoais no contexto da segurança pública. Por meio das exposições realizadas, a sociedade pode obter um conhecimento maior acerca da aplicação das normas de proteção de dados no setor e principalmente atentar para uma maior discussão legislativa e regulatória nessa área, tendo em vista sua urgência.

3. SÍNTESE DOS DEBATES

As discussões feitas durante o workshop foram sistematizadas abaixo:

Manifestação (posicionamento ou proposta).	Consenso, ponto a aprofundar ou dissenso.	Observações e comentários.
GUSTAVO RAMOS RODRIGUES (TERCEIRO SETOR).		
O moderador do workshop iniciou as discussões comentando sobre a exceção do artigo 4º da Lei Geral de Proteção de Dados, que remota a uma futura legislação específica a questão do tratamento de dados no setor de segurança pública.	Ponto a aprofundar.	s/o.
MILENA SANTANA DE ARAÚJO LIMA (SETOR GOVERNAMENTAL).		
O Regulamento 679 da União Europeia aborda sobre a questão de tratamento de dados e segurança pública. A painelistra sustenta que podemos usar essa solução como um referencial, mas que uma solução de segurança pública deve ser debatida, pensada e construída para a nossa realidade.	Ponto a aprofundar.	Na União Europeia, o sistema Schengen regula sobre o sistema de troca de informações entre os países-membro da União Europeia. No Brasil, possuímos entres federativos que tem bases de dados diferentes. A experiência do sistema Schengen pode servir para imaginar como podemos regulamentar a segurança pública no Brasil (PAULO SANTARÉM).
Acerca das tecnologias de reconhecimento facial, devemos encarar as pessoas não só como suspeitos, mas também como potenciais vítimas, que podem ser auxiliados pelo uso dessas tecnologias. O argumento é de que não podemos querer banir, via de regra, qualquer tipo de tecnologia, e sim pensar em como ela deve ser aplicada.	Ponto a aprofundar.	s/o.
Sobre a Autoridade Nacional de Proteção de Dados, a painelistra levanta a seguinte questão: haverá uma Autoridade Nacional única ou haverá uma Autoridade focada especificamente na questão da segurança pública?	Ponto a aprofundar.	Para aumentar o nível de confiança no poder público, a polícia pode indicar encarregados de proteção de dados (JACQUELINE ABREU).
Perante a discussão realizada, a painelistra sustenta que, em geral, devemos pensar, como sociedade, em qual modelo de segurança pública queremos construir. Esta seria, portanto, uma discussão que vai além da LGPD.	Ponto a aprofundar.	s/o.
Análises preventivas de crimes também podem ser utilizadas para a construção de políticas públicas, de forma que beneficiem a sociedade.	Dissenso.	Quando tratamos de análise preventiva de crimes no âmbito de políticas públicas, devemos ter em mente as salvaguardas que a LGPD e a própria Constituição Federal trazem para os cidadãos (BRUNA SANTOS).

PAULO RENÁ SANTARÉM (COMUNIDADE CIENTÍFICA E TECNOLÓGICA).

Os instrumentos legais de segurança pública (atualmente) respeitam dados pessoais? Questões primitivas do Direito retornam. Até onde a Polícia, o Judiciário, o Ministério Público pode ir? Não podemos nos desconectar das questões de direitos fundamentais ao pensar em proteção de dados.	Ponto a aprofundar.	s/o.
Sofremos com a ausência de dados empíricos e referências para entender como efetivamente é o setor de segurança pública no Brasil. “Quantas investigações dão certo ou não dão certo? Quais são aquelas que não alcançam êxito por falta de tratamento de dados pessoais?” O poder público quer justificar o tratamento de cada vez mais dados, mas sem apresentar resultados. Como avaliar o cenário da segurança pública no Brasil com a LGPD se o cenário atual não está disponível?	Ponto a aprofundar.	Como não temos tantos dados de realidade, o foco que podemos ter agora é nas normas. Pra melhorar a parte normativa, do dever ser. Podemos firmar compromissos com a legislação futura com a vinculação com princípios internacionais sobre aplicação de direitos humanos na vigilância das comunicações (PAULO SANTARÉM).
Na União Europeia, o sistema Schengen regula sobre o sistema de troca de informações entre os países-membro da União Europeia. No Brasil, possuímos entres federativos que tem bases de dados diferentes. A experiência do sistema Schengen pode servir para apoiar a construção de um modelo brasileiro.	Ponto a aprofundar.	s/o.
Quando falamos em dignidade da pessoa humana, temos que estabelecer compromissos legais claros, pois é um termo que aceita muitas interpretações.	Ponto a aprofundar.	s/o.

JACQUELINE DE SOUZA ABREU (SETOR PRIVADO).

A palestrante apresentou um organograma de como é o cenário hoje em aspectos legislativos, apresentando as principais leis sobre quebra de sigilo na investigação penal. A seguir, apresentou o novo paradigma criado pela Lei Geral de Proteção de Dados, problematizando os conceitos e definições da lei, que geram incertezas.	Ponto a aprofundar.	s/o.
A palestrante destacou que no modelo europeu, a regulações das atividades para essas finalidades foram aprovadas em conjunto com a GDPR, com a Diretiva 680.	Ponto a aprofundar.	s/o.
Alguns pontos da LGPD geram incertezas no setor privado. Por exemplo, as empresas do setor privado serão abrangidas por algumas exceções do tratamento de dados para finalidades do serviço público, quando feitas por empresas privadas? Além disso, o setor público frequentemente	Consenso.	Regras mais claras devem ser estabelecidas para o compartilhamento de dados entre setor público e setor privado.

requisita dados das empresas sem haver previsão legal.		
Como o setor de segurança pública vai se estruturar perante as obrigações de gerar relatórios de impacto?	Ponto a aprofundar.	s/o.

BRUNA MARTINS DOS SANTOS (TERCEIRO SETOR)

A palestrante comentou sobre diversos casos concretos de implementação de tecnologia e compartilhamento de dado pessoais no setor de segurança pública, evidenciando a falta de transparência para os titulares de dados e à população em geral acerca do tratamento desses dados.	Consenso.	s/o.
Frequentemente, o Estado encontra-se relativizando a ponderação de princípios, colocando a segurança pública na frente da privacidade.	Consenso.	Uma lei que trate de segurança pública e dados pessoais tem que ser proporcional ao ordenamento jurídico brasileiro e deve pensar em princípios constitucionais, respeitando-os (BRUNA SANTOS).
Soluções de tecnologias deveriam se pautar em questões de Direitos Humanos em sua concepção (Human rights by design).	Consenso.	s/o.
É necessário se pensar em em regulações específicas como <i>hacking</i> e <i>malware</i> .	Consenso.	É preciso pensar em boas definições de aspectos tecnológicos para as legislações acerca de tecnologia.

PERGUNTAS DO PÚBLICO

PERGUNTAS	COMENTÁRIOS DOS PAINELISTAS
1) Quais são os riscos de uma privatização do DATAPREV tendo em vista o escândalo da Cambridge Analytica?	Sobre a possibilidade de agentes privados serem utilizados na segurança pública: Será que isso é comum na segurança pública no Brasil? Não temos normas claras para definir o que são os abusos, o que dirá avaliar quais são os abusos. Os problemas de privacidade não são inicialmente percebidos. (PAULO SANTARÉM).
2) As forças de segurança pública do país estão prontas para lidar com a LGPD? E quem da parcela da população está mais vulnerável?	Os segmentos sociais mais vulneráveis com certeza serão mais vulnerabilizados. Pessoas com menos poder de barganha podem ser alvo central de políticas públicas malconduzidas (PAULO SANTARÉM). A segurança pública, independente da LGPD, já trata dados. A lei não aumenta o poder público, mas pode limitá-lo (MILENA LIMA). Para crescer o nível de confiança no tratamento de dados, a polícia poderia apontar um encarregado de proteção de dados para definir limites. Precisamos avaliar a tecnologia para tentar entender os impactos (JACQUELINE ABREU).

	<p>Algumas bases de dados do governo não tem um sistema de segurança robusto o suficiente. Temos que ter garantias de que as informações das bases governamentais não serão vazadas (BRUNA SANTOS).</p>
<p>3) A tecnologia pode fazer uma segregação pelo reconhecimento facial? E qual o conceito de segurança pública da lei?</p>	<p>Não necessariamente vai segregar alguém, pois o trabalho da polícia é apurar os fatos (MILENA LIMA).</p> <p>Alguns sistemas de reconhecimento facial tem viés de algoritmo e não deveriam ser utilizados em larga escala em políticas públicas (BRUNA SANTOS).</p>
<p>4) E se fosse concretizada a proposta de que a Autoridade Nacional analisasse as tecnologias antes delas entrarem no mercado?</p>	<p>Será que há espaço político real para avaliarmos tecnologias no poder privado? Alteração das tecnologias já existe, isso seria uma espécie de censura e facilmente contornável. Essa seria uma medida prudente, mas que não é aceitável. (PAULO SANTARÉM)</p> <p>Essa seria uma questão complicada pois pode servir como censura, ofensa à liberdade de expressão e iniciativa mas precisamos de um compromisso da Autoridade para poder averiguar as tecnologias para entender os seus impactos (JAQUELINE ABREU).</p>